

THE ASSISTANT COMMISSIONER OF PATENTS
Washington, D.C. 20231

DOCKET NUMBER: RP9-98-089
March 3, 1999

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventor: **David C. Challener et al.**

For: **DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE USER PRIVATE KEYS IN NON-SECURE STORAGE**

Enclosed are:

- ☒ Patent Specification and Executed Declaration
- ☒ Five sheets of drawing(s).
- ☒ An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).
- ☐ A certified copy of a ___ application.
- ☐ Information Disclosure Statement, PTO 1449 and copies of references.

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				\$760.00
Total Claims	17	- 20	x 18 =	\$
Indep. Claims	3	- 3	x 78 =	\$
MULTIPLE DEPENDENT CLAIM PRESENTED			x 260 =	\$
			TOTAL	\$760.00

- ☒ Please charge my IBM Corporation Deposit Account No. 50-0563 in the amount of \$760.00. A duplicate copy of this sheet is enclosed.
- ☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to IBM Corporation Deposit Account 50-0563. A duplicate copy of this sheet is enclosed.
- ☒ Any additional filing fees required under 37 CFR §1.16.
- ☒ Any patent application processing fees under 37 CFR §1.17.

CERTIFICATE OF MAILING BY "EXPRESS MAIL" UNDER 37 CFR § 1.10

"Express Mail" mailing label number **EL281538455US**

Date of Mailing. **March 3, 1999**

I hereby certify that the documents indicated below are being deposited with the United States Postal Service under 37 CFR 1.10 on the date indicated above and are addressed to Box Patent Applications, Assistant Commissioner of Patents, Washington, D.C. 20231 and mailed on the above Date of Mailing with the above "Express Mail" mailing label number

Eric Ha

(name of person mailing paper)

SIGNATURE of person mailing paper or fee

Respectfully submitted,

By

Andrew J. Dillon

Registration No. 29,634

FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP
Suite 350, Lakewood on the Park
7600B North Capital of Texas Highway
Austin, Texas 78731
Telephone (512) 343-6116

DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE
USER PRIVATE KEYS IN NON-SECURE STORAGE

Background of the Invention

1. Field of the Invention:

5 The present invention relates in general to data processing systems and, in particular, to a data processing system and method for maintaining multiple, secure private keys in a non-secure storage device. Still more particularly, the present invention relates to a data
10 processing system and method for maintaining multiple, secure private keys in a non-secure storage device by encrypting the private keys utilizing a master public key stored in protected storage prior to storing the user private keys in the non-secure storage device.

15 **2. Description of the Related Art:**

 Personal computer systems are well known in the art. They have attained widespread use for providing computer power to many segments of today's modern society. Personal computers (PCs) may be defined as a desktop, floor standing, or portable microcomputer that includes a system unit having
20 a central processing unit (CPU) and associated volatile and non-volatile memory, including random access memory (RAM) and basic input/output system read only memory (BIOS ROM), a system monitor, a keyboard, one or more flexible diskette
25 drives, a CD-ROM drive, a fixed disk storage drive (also known as a "hard drive"), a pointing device such as a mouse, and an optional network interface adapter. One of the distinguishing characteristics of these systems is the use of a motherboard or system planar to electrically connect

these components together. Examples of such personal computer systems are IBM's PC 300 series, Aptiva series, and Intellistation series.

5 Encryption algorithms are known to ensure that only the intended recipient of a message may read and access the message. One known encryption algorithm is an asymmetric, or public key, algorithm. The public key algorithm is a method for encrypting messages sent from a first computer system to a second computer system. This algorithm provides
10 for a key pair including a public key and a private key for each participant in a secure communication. This key pair is unique to each participant. An example of such an encryption scheme is an RSA key pair system.

15 Prior to the first computer system transmitting a message, the first computer system obtains the public key of the intended recipient of the message, in this case the second computer system. The public key of the second system is obtained by the first computer system from the second computer system. The first computer system then encrypts
20 the message using the public key of the second computer system. The message is then transmitted to the computer identified by the public key, i.e. the second computer system. Upon receipt of the message, the second computer utilizes its private key to decrypt the message.

25 A key pair is also typically established for each user within a computer system for each application. A user may be a person, a device, an application, or anything else that may access an application. Therefore, many key pairs must be maintained by a computer system. Protected storage is
30 required to store the key pairs. The protected storage is typically a storage device having very limited storage space. Because it takes a large number of bytes of

protected storage to store a single RSA key, it is impractical to maintain multiple private keys in the protected storage.

Therefore a need exists for a data processing system and method for maintaining multiple, secure private keys in non-secure storage.

5

SUMMARY OF THE INVENTION

A data processing system and method are disclosed for maintaining secure user private keys in a non-secure storage device. A master key pair is established for the system. The master key pair includes a master private key and a master public key. The master key pair is stored in a protected storage device. A unique user key pair is established for each user. The user key pair includes a user private key and a user public key. The user private key is encrypted utilizing the master public key. The encrypted user private key is stored in the non-secure storage device, wherein the encrypted user private key is secure while stored in the non-secure storage device.

The above as well as additional objectives, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features are set forth in the appended claims. The present invention itself, however, as well as a preferred mode of use, further objectives, and advantages thereof, will best be understood by reference to the following detailed description of a preferred embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 illustrates a pictorial representation of a data processing system capable of maintaining multiple, secure private keys in non-secure storage in accordance with the method and system of the present invention;

Figure 2 depicts a more detailed pictorial representation of the data processing system of **Figure 1** in accordance with the method and system of the present invention;

Figure 3 illustrates a high level flow chart which depicts establishing and storing a master key pair in protected storage in a data processing system in accordance with the method and system of the present invention;

Figure 4 depicts a high level flow chart which illustrates establishing and storing multiple, secure user private keys in non-secure storage in a data processing system in accordance with the method and system of the present invention; and

Figure 5 illustrates a high level flow chart which depicts an application utilizing an encrypted user private key for cryptographic services in accordance with the method and system of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

A preferred embodiment of the present invention and its advantages are better understood by referring to Figures 1-5 of the drawings, like numerals being used for like and corresponding parts of the accompanying drawings.

The present invention is a method and system for maintaining multiple, secure user private keys in a non-secure storage device. Before storing the user private keys, the user private key is first encrypted utilizing a master key pair stored in protected storage. The master key pair is associated with only the system which generated the master key pair. A master key pair includes a master private key and a master public key. Preferably, only the master public key is utilized to encrypt the user key pair.

An RSA encrypted user private key is stored in a protected storage device within an encryption device. When the master public key is utilized to encrypt a message, only the master private key may be utilized to decrypt the message. Because the master private key is not made available, either to the system itself or a user, no other system or user will be able to decrypt the user private keys encrypted with the master public key. Therefore, the encrypted user private keys are secure even when they are stored in non-secure storage.

Each user within the system has a separate, unique user key pair established for each application within the system. The term "user" is understood to mean a person, a service, an application, a device, or any other entity which may access an application. The term "user" is not limited to a

human user. Therefore, a user key pair is associated with a particular user and a particular application.

A certificate may be established within the system for a user to access a particular application. The certificate is established for and associated with a particular user and a particular application. The certificate includes a pointer to its associated application, an identity of the user associated with the user key pairs and this certificate, and a pointer to the user private key associated with this user and application. The application associated with a particular certificate may need to transmit a message encrypted utilizing this user's private key. The encryption engine included with the system accesses the user private key pointed to by the certificate. The encryption engine, then, decrypts the user private key. The message is encrypted by the encryption engine utilizing the decrypted user private key, and then transmitted.

Figure 1 illustrates a pictorial representation of a data processing system capable of maintaining multiple, secure user private keys in a non-secure storage device in accordance with the method and system of the present invention. Computer system 30 includes a computer 12, a monitor 13, a keyboard 14, and a printer or plotter 15. Computer system 30 may be implemented utilizing any commercially available computer system which has been suitably programmed and which has been modified as described below.

Figure 2 depicts a more detailed pictorial representation of the data processing system of **Figure 1** in accordance with the method and system of the present invention. Computer 12 includes a planar (also commonly called a motherboard or system board) which is mounted

within computer 12 and provides a means for mounting and electrically interconnecting various components of computer 12 including a central processing unit (CPU) 200, system memory 206, and accessory cards or boards as is well known in the art.

CPU 200 is connected by address, control, and data busses 202 to a memory controller and peripheral component interconnect (PCI) bus bridge 204 which is coupled to system memory 206. An integrated drive electronics (IDE) device controller 220, and a PCI bus to Industry Standard Architecture (ISA) bus bridge 204 are connected to PCI bus bridge 204 utilizing PCI bus 208. IDE controller 220 provides for the attachment of IDE compatible storage devices, such a removable hard disk drive 222. PCI/ISA bridge 212 provides an interface between PCI bus 208 and an optional feature or expansion bus such as the ISA bus 214. PCI/ISA bridge 212 includes power management logic. PCI/ISA bridge 212 is supplied power from battery 244 to prevent loss of configuration data stored in CMOS 213.

A PCI standard expansion bus with connector slots 210 is coupled to PCI bridge 204. PCI connector slots 210 may receive PCI bus compatible peripheral cards. An ISA standard expansion bus with connector slots 216 is connected to PCI/ISA bridge 212. ISA connector slots 216 may receive ISA compatible adapter cards (not shown). It will be appreciated that other expansion bus types may be used to permit expansion of the system with added devices. It should also be appreciated that two expansion busses are not required to implement the present invention.

An I/O controller 218 is coupled to PCI-ISA bridge controller 212. I/O controller 218 controls communication between PCI-ISA bridge controller 212 and devices and

peripherals such as floppy drive 224, keyboard 14, and mouse 228 so that these devices may communicate with CPU 200.

PCI-ISA bridge controller 212 includes an interface for a flash memory 242 which includes an interface for address, data, flash chip select, and read/write. Flash memory 242 is an electrically erasable programmable read only memory (EEPROM) module and includes BIOS that is used to interface between the I/O devices and operating system.

Computer 12 includes a video controller 246 which may, for example, be plugged into one of PCI expansion slots 210. Video controller 246 is connected to video memory 248. The image in video memory 248 is read by controller 246 and displayed on monitor 13 which is connected to computer 12 through connector 250.

Computer system 12 includes a power supply 240 which supplies full normal system power 243, and has an auxiliary power main AUX 5 241 which supplies full time power to the power management logic 212.

In accordance with the present invention, planar includes a security ASIC 261 which includes an encryption/decryption engine 260 which includes an encryption/decryption algorithm which is utilized to encode and decode messages transmitted and received by the planar, and protected storage 262. Engine 260 can preferably perform public\private key encryption. Engine 260 may access a protected storage device 262. Protected storage device 262 is accessible only through engine 260, and is a one-time writable device. Therefore, storage device 262 cannot be read or written to by the planar, device 222, or any other device. Keys stored within storage 262 are protected by engine 260 and are not accessible to the planar

or its components. Storage device 262 is utilized to store the master key pair, including the master private key and master public key. Because keys require a large amount of storage and the limited storage space within storage device 262, it is not practical to store multiple user private keys in storage device 262. Device 262 may be implemented utilizing an electronically erasable storage device, such as an EEPROM. Access may be gained to non-readable storage device 262 in order to initially store the master private key. However, after the master private key is stored, it cannot be read. The keys stored in EEPROM 262 may not be read by any component of the planar other than engine 260.

ASIC 261, including engine 260 and EEPROM 262, is coupled to PCI-ISA bridge 212 utilizing a system management (SM) bus 238. System management bus 238 is a two-wire, low speed, serial bus used to interconnect management and monitoring devices. Those skilled in the art will recognize that ASIC 261 may be coupled to another bus within the planar.

Figure 3 illustrates a high level flow chart which depicts establishing and storing a master key pair in protected storage in a data processing system in accordance with the method and system of the present invention. The process starts as depicted at block 300 and thereafter passes to block 302 which illustrates establishing a master key pair for data processing system 30. Next, block 304 depicts the storage of the master public key and master private key in protected storage 262 which is a one-time writable, protected storage. The process then terminates as illustrated at block 306.

Figure 4 depicts a high level flow chart which illustrates establishing and storing multiple, secure user

private keys in non-secure storage in a data processing system in accordance with the method and system of the present invention. The process starts as illustrated at block 400 and thereafter passes to block 402 which depicts a creation of a user key pair for each user. Next, block 404 illustrates the encryption of each user private key utilizing the master public key. Block 406, then, depicts the storage of each encrypted user private key in the hard drive or other storage. The user private keys encrypted by a particular data processing system are not capable of being utilized by other data processing systems. The process then passes to block 408 which illustrates establishing a certificate for accessing applications. A certificate includes a pointer to the application, a pointer to storage to locate the user private key for this application for this particular user, and an identifier which identifies this particular user. Thereafter, block 410 depicts the storage of the certificate in the hard drive or other storage. The process then terminates as depicted at block 412.

Figure 5 illustrates a high level flow chart which depicts an application utilizing an encrypted user private key for cryptographic services in accordance with the method and system of the present invention. The process starts as illustrated at block 500 and thereafter passes to block 502 which depicts a user selecting a particular certificate. The certificate is associated this user and with a particular application. It points to this user's encrypted user private key for the particular application. Thereafter, block 504 illustrates the encryption engine decrypting the user private key using the master private key. The encryption engine does not make the decrypted user private key available to any service, application, or device. Next, block 506 depicts the application associated with this certificate using the encryption engine and the

user key pair for cryptographic services. The process then terminates as depicted at block 508.

5 While a preferred embodiment has been particularly shown and described, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the present invention.

FIG. 10 is a block diagram of a system for providing a user with a secure communication channel. The system includes a user device 100, a network 102, and a server 104. The user device 100 is connected to the network 102, which is connected to the server 104. The server 104 is configured to provide a secure communication channel to the user device 100. The user device 100 is configured to receive a secure communication channel from the server 104. The network 102 is configured to provide a secure communication channel to the user device 100. The server 104 is configured to provide a secure communication channel to the user device 100.

CLAIMS:

1 1. A method in a data processing system for maintaining
2 secure user private keys in a non-secure storage device,
3 said method comprising the steps of:

4 establishing a master key pair for said system, said
5 master key pair including a master private key and a master
6 public key;

7 storing said master key pair in a protected storage
8 device;

9 establishing a unique user key pair for a user, said
10 user key pair including a user private key and a user public
11 key;

12 encrypting said user private key utilizing said master
13 public key; and

14 storing said encrypted user private key in said non-
15 secure storage device, wherein said encrypted user private
16 key is secure while stored in said non-secure storage
17 device.

1 2. The method according to claim 1, further comprising the
2 steps of:

3 establishing an encryption device having an encryption
4 engine and said protected storage device; and

5 said protected storage device being accessible only
6 through said encryption engine.

1 3. The method according to claim 2, further comprising the
2 step of said encryption engine encrypting said user private
3 key utilizing said master public key stored in said
4 protected storage device.

1 4. The method according to claim 3, further comprising the
2 steps of:

3 an application generating a message to transmit to a
4 recipient;

5 said encryption engine decrypting said user private key
6 utilizing said master private key;

7 said encryption engine encrypting said message
8 utilizing said decrypted user private key and a recipient's
9 public key; and

10 said system transmitting said encrypted message to said
11 recipient.

12 5. The method according to claim 4, wherein the step of
2 establishing a user key pair further comprises the step of
3 associating said user key pair with an application.

1 6. The method according to claim 5, further comprising the
2 steps of:

3 establishing a certificate, said certificate being
4 associated with said application, said user private key, and
5 said user;

6 in response to said user attempting to access said
7 application utilizing said certificate, said encryption
8 engine utilizing said certificate to determine a location
9 within said non-secure storage device for said user private
10 key associated with said certificate;

11 said encryption engine decrypting said user private
12 key; and

13 said encryption engine utilizing said decrypted user
14 private key to encrypt messages transmitted by said
15 application.

1 7. The method according to claim 6, wherein said step of
2 storing said user private key in said non-secure storage
3 further comprises the step of storing said user private key
4 in a hard drive.

1 8. The method according to claim 7, further comprising the
2 step of said user key pair being capable of being utilized
3 only in said data processing system wherein said user key
4 pair is established, wherein said user key pair is not
5 capable of being utilized in a second data processing
6 system.

1 9. A data processing system for maintaining secure user
2 private keys in a non-secure storage device, comprising:

3 an encryption device included within said system for
4 establishing a master key pair for said system, said master
5 key pair including a master private key and a master public
6 key;

7 a protected storage device for storing said master key
8 pair;

9 said encryption device executing code for establishing
10 a unique user key pair for a user, said user key pair
11 including a user private key and a user public key;

12 said encryption device executing code for encrypting
13 said user private key utilizing said master public key; and

14 said non-secure storage device for storing said
15 encrypted user private key, wherein said encrypted user
16 private key is secure while stored in said non-secure
17 storage device.

1 10. The system according to claim 9, further comprising:

2 said encryption device including an encryption engine
3 and said protected storage device; and

4 said protected storage device capable of being accessed
5 only through said encryption engine.

1 11. The system according to claim 10, further comprising
2 said encryption engine executing code for encrypting said
3 user private key utilizing said master public key stored in
4 said protected storage device.

1 12. The system according to claim 11, further comprising:

2 an application capable of generating a message to
3 transmit to a recipient;

4 said encryption engine executing code for decrypting
5 said user private key utilizing said master private key;

6 said encryption engine executing code for encrypting
7 said message utilizing said decrypted user private key and a
8 recipient's public key; and

9 said system transmitting said encrypted message to said
10 recipient.

11 13. The system according to claim 12, further comprising
12 said system executing code for associating said user key
13 pair with an application.

1 14. The system according to claim 13, further comprising:

2 said system executing code for establishing a
3 certificate, said certificate being associated with said
4 application, said user private key, and said user;

5 in response to said user attempting to access said
6 application utilizing said certificate, said encryption
7 engine executing code utilizing said certificate for
8 determining a location within said non-secure storage device
9 for said user private key associated with said certificate;

10 said encryption engine executing code for decrypting
11 said user private key pair; and

12 said encryption engine capable of utilizing said
13 decrypted user private key to encrypt messages transmitted
14 by said application.

15 15. The system according to claim 14, further comprising
16 said system executing code for storing said user private key
17 in a hard drive.

1 16. The system according to claim 15, further comprising
2 said user key pair being capable of being utilized only in
3 said data processing system wherein said user key pair is
4 established, wherein said user key pair is not capable of
5 being utilized in a second data processing system.

1 17. A data processing system for maintaining secure user
2 private keys in a non-secure hard drive, comprising:

3 an encryption device including an encryption engine and
4 a protected storage device for establishing a master key
5 pair for said system, said master key pair including a
6 master private key and a master public key, said protected
7 storage device for storing said master key pair, said
8 protected storage device capable of being accessed only
9 through said encryption engine;

10 said encryption device executing code for establishing
11 a unique user key pair for a user, said user key pair
12 including a user private key and a user public key, said
13 user key pair being capable of being utilized only in said
14 data processing system wherein said user key pair is
15 established, wherein said user key pair is not capable of
16 being utilized in a second data processing system;

17 said system executing code for associating said user
18 key pair with an application;

19 said encryption device executing code for encrypting
20 said user private key utilizing said master private key
21 stored in said protected storage device;

22 said non-secure hard drive for storing said encrypted
23 user private key, wherein said encrypted user private key is
24 secure while stored in said non-secure hard drive;

25 an application capable of generating a message to
26 transmit to a recipient;

27 said system executing code for establishing a
28 certificate, said certificate being associated with said
29 application, said user private key, and said user;

30 storing said certificate in said non-secure hard drive;

31 in response to said user attempting to access said
32 application utilizing said certificate, said encryption
33 engine executing code utilizing said certificate for
34 determining a location within said non-secure hard drive for
35 said user private key associated with said certificate;

36 said encryption engine executing code for decrypting
37 said user private key;

38 said encryption engine capable of utilizing said
39 decrypted user private key to encrypt messages transmitted
40 by said application; and

41 said system transmitting said encrypted message to said
42 recipient.

ABSTRACT OF THE DISCLOSURE

DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE
USER PRIVATE KEYS IN NON-SECURE STORAGE

1 A data processing system and method are disclosed for
2 maintaining secure user private keys in a non-secure storage
3 device. A master key pair is established for the system. The
4 master key pair includes a master private key and a master
5 public key. The master key pair is stored in a protected
6 storage device. A unique user key pair is established for
7 each user. The user key pair includes a user private key and
8 a user public key. The user private key is encrypted
9 utilizing the master public key. The encrypted user private
10 key is stored in the non-secure storage device, wherein the
11 encrypted user private key is secure while stored in the non-
12 secure storage device.

30

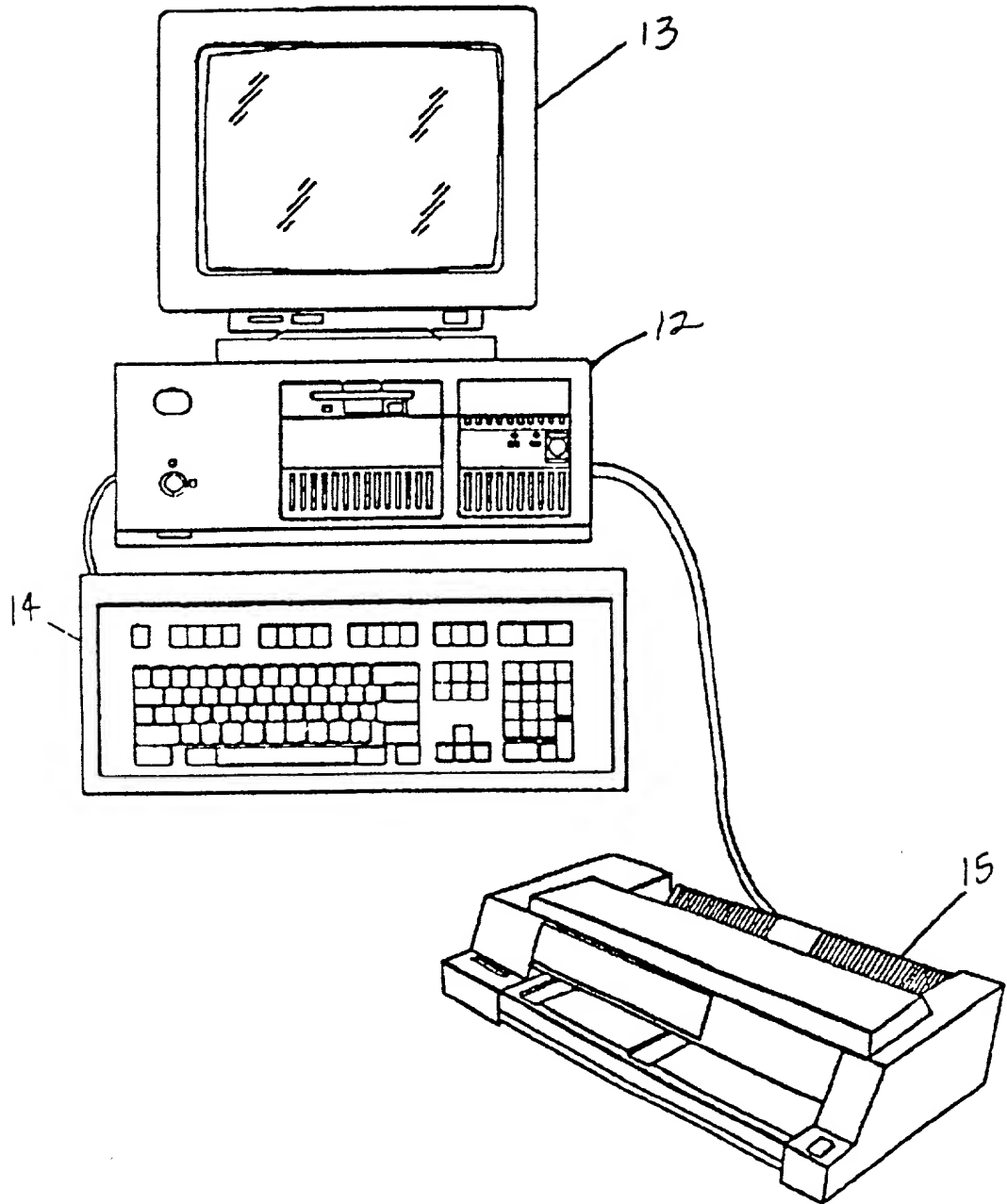


Fig. 1

RP998089

RP9-98-089

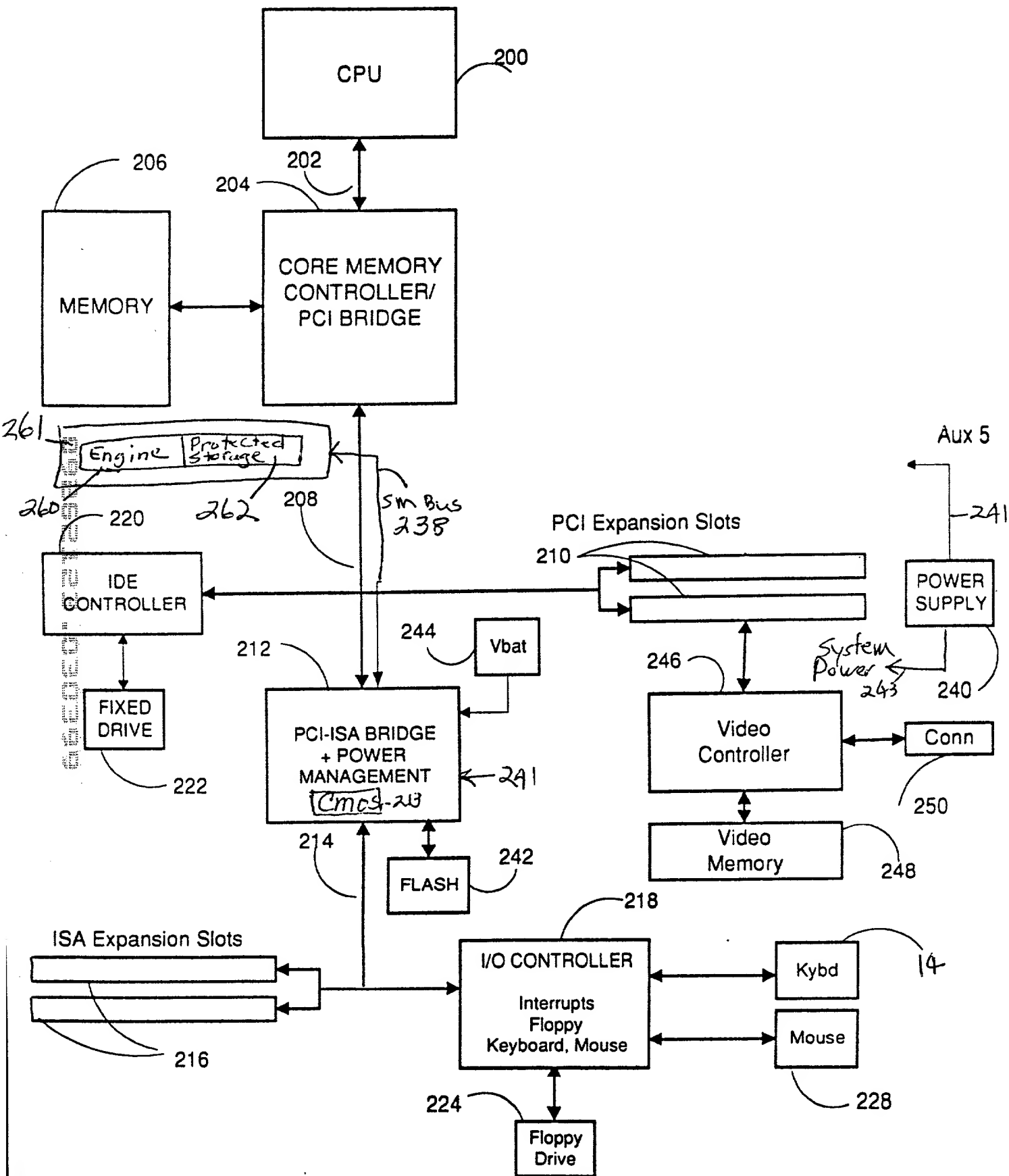


Fig. 2

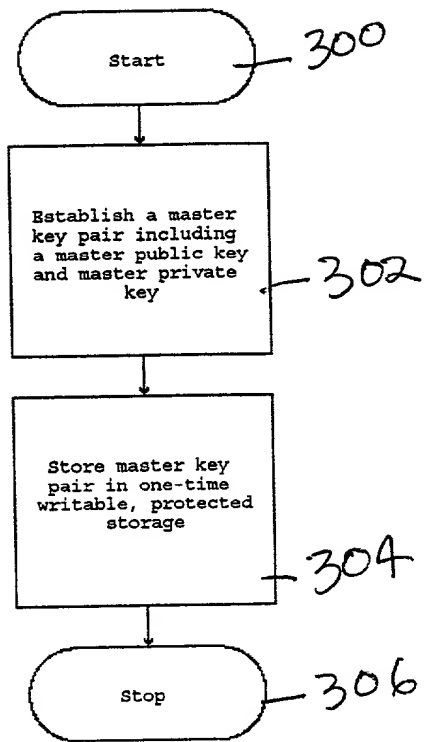


Fig. 3

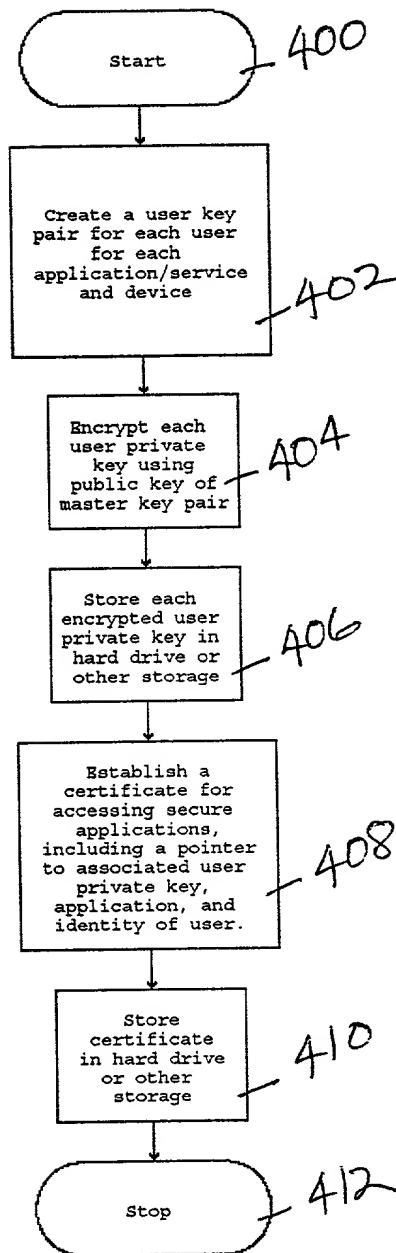


Fig. 4

RP998089

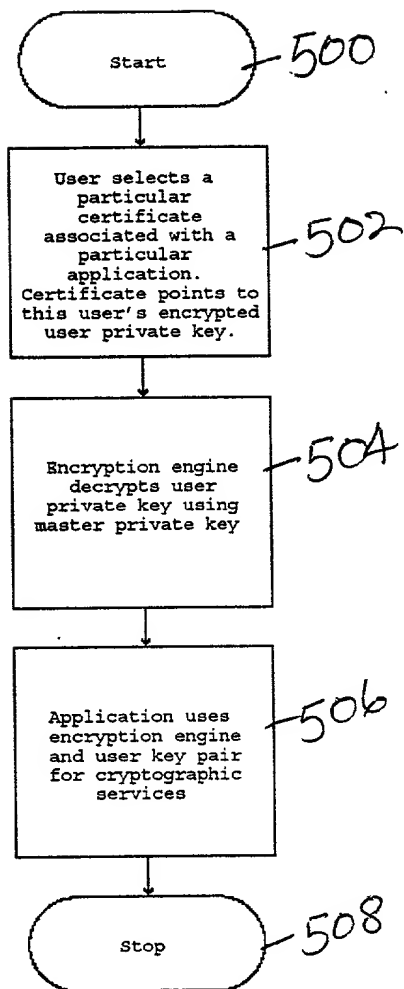


Fig. 5

RP998089

**DECLARATION AND POWER OF ATTORNEY FOR
PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE
USER PRIVATE KEYS IN NON-SECURE STORAGE**

the specification of which (check one)

X is attached hereto.

— was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):	Priority Claimed
_____	___ Yes___ No
(Number) (Country) (Day/Month/Year)	

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____	_____	_____
(Application Serial #)	(Filing Date)	(Status)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and

further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Horace St. Julian, Reg. No. 30,329; Bernard D. Bogdon, Reg. No. 27,773; George E. Grosser, Reg. No. 25,629; Anthony N. Magistrale, Reg. No. 35,595; Daniel E. McConnell, Reg. No. 20,360; Martin J. McKinley, Reg. No. 31,782; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Matthew W. Bace, Reg. No. 42,277; Max Cicccarelli, Reg. No. 39,454; Andrew J. Dillon, Reg. No. 29,634; Justin M. Dillon, Reg. No. 42,486; John G. Graham, Reg. No. 19,563; Kenneth C. Hill, Reg. No. 29,650; Melvin A. Hunn, Reg. No. 32,574; Jack V. Musgrove, Reg. No. 31,986; Antony P. Ng, Reg. No. 43,032; Brian F. Russell, Reg. No. 40,796; Daniel E. Venglarik, Reg. No. 39,409; and Philip T. Virga, Reg. No. 36,710.

Send correspondence to: Andrew J. Dillon, FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Suite 350, Lakewood on the Park, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon, (512) 343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: David Carroll Challener

INVENTORS SIGNATURE: David Carroll Challener DATE: 2/25/1999

RESIDENCE: 713 Hunting Ridge Road
Raleigh, North Carolina 27615

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 713 Hunting Ridge Road
Raleigh, North Carolina 27615

FULL NAME OF SECOND INVENTOR: Daryl Carvis Cromer

INVENTORS SIGNATURE: Daryl Carvis Cromer DATE: 2/24/99

RESIDENCE: 2631 Grande Valley Circle Drive
Cary, North Carolina 27513

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 2631 Grande Valley Circle Drive
Cary, North Carolina 27513

DOCKET NUMBER: RP9-98-089

FULL NAME OF THIRD INVENTOR: Mark Charles Davis

INVENTORS SIGNATURE: Mark Charles Davis DATE: 3/1/99

RESIDENCE: 201 Spring Garden Drive
Durham, North Carolina 27713-7533

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 201 Spring Garden Drive
Durham, North Carolina 27713-7533

FULL NAME OF FOURTH INVENTOR: Howard Locker

INVENTORS SIGNATURE: Howard Locker DATE: 2/24/99

RESIDENCE: 103 Paladin Place
Cary, North Carolina 27513

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 103 Paladin Place
Cary, North Carolina 27513

FULL NAME OF FIFTH INVENTOR: Andy Lloyd Trotter

INVENTORS SIGNATURE: Andy Lloyd Trotter DATE: 02/29/99

RESIDENCE: 8203-107 Green Lantern Street
Raleigh, North Carolina 27613

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 8203-107 Green Lantern Street
Raleigh, North Carolina 27613

FULL NAME OF SIXTH INVENTOR: James Peter Ward

INVENTORS SIGNATURE: James Peter Ward DATE: 2/24/99

RESIDENCE: 107 Hemingway Forst Place
Raleigh, North Carolina 27607

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 107 Hemingway Forst Place
Raleigh, North Carolina 27607